BELMONT
PRIMARY SCHOOL
Inspire ~ Nurture ~ Flourish

E-Safety Handbook

Belmont Primary School acknowledges the assistance of Becta, SWGfL, Kent County Council & Sheffield Children and Young Peoples' Directorate in providing content in this document.

This handbook should be read in conjunction with other policies including those for Safeguarding and Child Protection, Behaviour and Teaching and Learning.

Throughout this handbook 'parents' denotes those with parental responsibility.

Contents

PART ONE - E-SAFETY POLICY

PART TWO - HANDBOOK

PART ONE - E-SAFETY POLICY

1. Mission Statement

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. Belmont Primary School makes full use of these technologies to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. We believe access to the Internet is an entitlement for pupils who show a responsible and mature approach to its use and that the School has a duty to provide pupils with quality Internet access. The School also recognises that pupils will use these technologies outside school and need to learn how to take care of their own safety and security. Belmont Primary School fully recognises its responsibilities for e-safety, including a responsibility to educate our pupils about the benefits and risks of using new technology and the provision of safeguards and information for all users to enable them to control their online experiences.

This Policy applies to all members of the school community (including staff, pupils, volunteers, parents, visitors, community users) who have access to and are users of school Information and Communication Technology (ICT) systems, both in and out of school. All adults, including volunteers, working in or on behalf of the School share the responsibility to keep children safe from harm

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this Policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour that take place out of school.

1.1 Aims and objectives

Our School aims to ensure that children are effectively safeguarded from potential risk of harm and that the safety and well-being of children is of the highest priority in all aspects of the School's work.

Specifically we aim to:

- ensure that all stakeholders are aware of and take seriously their responsibility to promote and safeguard the online safety of children;
- use the Internet and other technologies as tools for teaching and learning within the context of educating children and adults in how to use such technology responsibly, giving clear expectations for appropriate use;
- ensure staff and children understand the dangers that can arise and the procedures for dealing with e-safety incidents;
- ensure that school Internet access is appropriate for both pupil and adult use and includes filtering appropriate to the age of pupils;
- guide pupils in using technologies and developing skills in ways appropriate to their age and maturity.

2. Roles and Responsibilities

2.1 Governors

A member of the Governing Body has taken on the role of E-Safety Governor (Pat Devito, Deputy Child Protection Governor). Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the Policy. Review of effectiveness will be carried out by the governors receiving regular information about e-safety incidents and monitoring reports. The role of the E-Safety Governor includes:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety Incident Logs
- regular monitoring of Filtering/Change Control Logs
- reporting to the governors' Community Committee

2.2 Head Teacher and Senior Leaders

The Head Teacher (or in her absence the Deputy or another member of the Senior Leadership Team) is responsible for:

- ensuring the E-Safety Policy is disseminated and its importance explained;
- ensuring the safety (including e-safety) of members of the School Community (although the day today responsibility for e-safety is delegated to the E-Safety Co-ordinator);
- ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable continuing professional development (CPD) to enable them to carry out their e-safety roles and to train other colleagues, as is relevant;
- ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;
- receiving regular monitoring reports from the E-Safety Co-ordinator;
- having familiarity with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Head Teacher is designated person for child protection and as such should be

- trained in e-safety issues;
- aware of the potential for serious child protection issues to arise from: sharing of personal data; access to illegal/inappropriate materials; inappropriate online contact with adults/strangers; potential or actual incidents of grooming and cyber-bullying.

2.3 E-Safety Co-ordinator: Michelle Clifton

The E-Safety Co-ordinator has responsibility for:

- assisting the Head Teacher in making sure that the Policy is disseminated and clearly understood;
- taking day to day responsibility for e-safety issues and a leading role in establishing and reviewing the E-Safety Handbook;
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- providing training and advice for staff;
- liaising with the Local Authority;
- liaising with school ICT technical staff;
- receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments;
- meeting regularly with the E-Safety Governor to discuss current issues, review Incident Logs and Filtering/Change Control Logs;
- attending relevant meetings of the governors' Community Committee to give reports;
- reporting regularly to Senior Leadership Team;
- managing password security and allocating passwords for new users, and replacement passwords for existing users;
- carrying out an e-safety audit every two years and producing an action plan if necessary (refer to E- Safety Audit in E-Safety Handbook).

2.4 Network Manager

The Network Manager is responsible for ensuring that:

- the School's ICT infrastructure is secure and is not open to misuse or malicious attack with effective protection (e.g. firewall/anti-virus software) in place;
- the School meets the e-safety technical requirements outlined in any relevant Local Authority e-safety policy and guidance;
- users may only access the School's networks with allocated passwords, that are periodically changed;
- he/she keeps up to date with e-safety technical information in order to effectively carry out his/her e-safety role and to inform and update others as relevant;
- the use of the network, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator for investigation, action and/or sanction;
- the School's Filtering Policy (see section 10) is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- the school filtering system is effectively managed and records/logs are kept of changes and of breaches of the filtering systems;
- there is a system of checks and balances to protect those responsible, changes must be reported to a second responsible person (E-Safety Co-ordinator) every term in the form of an audit of the Change Control Logs.

2.5 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read, understood and signed the school Staff Acceptable Use Policy Agreement;
- they report any suspected misuse or problem to the E-Safety Co-ordinator;
- digital communications with pupils (email, voice, video) are only on a professional level and carried out using official school systems;
- e-safety issues are embedded in all aspects of the Curriculum and other school activities;
- pupils understand and follow the school E-Safety, Acceptable Use Policy and Google Classroom agreement;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extra-curricular and extended school activities;
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices, monitor their use and implement current school policies with regard to these devices;
- in lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches;
- they safeguard the security of their username and password and do not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security and MUST change their password immediately;
- they report immediately to the E-Safety Co-ordinator any infringements in the School's filtering of which they become aware or any sites that are accessed, which they believe should have been filtered;
- they do not attempt to use any programmes or software that might allow them to bypass the filtering or security systems in place to prevent access to such materials.
- they at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- they use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data;
- they will 'lock' computers when they are not in use using the Windows key + L.

2.6 Pupils

Pupils are expected to:

- use the school ICT systems in accordance with the Pupil Acceptable Use Policy and Google Classroom agreement;, which they will be required to agree to before being given access to school systems;
- report abuse, misuse or access to inappropriate materials, once they know how to do so;
- know and understand school policies and procedures on the use of mobile phones, digital cameras and hand held devices including the taking or use of images;
- understand that cyber-bullying is a form of bullying and will not be tolerated;
- safeguard the security of their username and password and not allow other users to access the systems using their log on details. They should report any suspicion or evidence that there has been a breach of security so their password can be changed;
- understand the importance of adopting good e-safety practice when using digital technologies out of school and recognise that the School's E-Safety Policy covers their actions out of school, if related to their membership of the School.

2.7 Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents do not fully understand the issues and are less experienced in the use of ICT than their children. The School will therefore take every opportunity to help parents understand these issues through e-safety evenings, newsletters, letters, website and information about national and local e-safety campaigns or literature.

Parents will be responsible for:

- endorsing the Pupil Acceptable Use Policy and Google Classroom agreement;
- accessing the school website in accordance with the relevant School Acceptable Use Policy.

3. E-Safety Education

The education of pupils in e-safety is an essential part of the school's e-safety provision. Children need the help and support of the School to recognise and avoid e-safety risks and build their resilience. E-Safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

E-Safety education is provided in the following ways:

- a planned e-safety programme is provided as part of Computing /PSHE and should be regularly revisited – this will cover the use of ICT and new technologies both in school and outside school (e-safety is taught using the CEOP 'Thinkuknow' resources);
- pupils are helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school;
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- rules for use of ICT systems and Internet are posted in all rooms;
- staff act as good role models in their use of ICT, the Internet and mobile devices;
- Parents have access to Parent Zone (an online e-safety resource the school has subscribed to).

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

(Also see Internet Access, World Wide Web, Use of Digital and Video Images, Use of email, Use of Social Networking).

4. Internet Access

- All staff must read and agree to the Acceptable Use Policy Agreement before using any School ICT resource.
- All pupils and parents will be asked to read and agree to an AUP form on entry to the school.
- Parents will be informed that pupils will be provided with supervised Internet access.
- School Policy restricts certain Internet usage (refer to the Restricted Internet Usage table in E-Safety Handbook page 13)

5. World Wide Web

- Belmont Primary School use a London Grid for Learning (LGfL) filtered Internet Service, which will minimise the chances of pupils encountering undesirable material. The School will normally only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff are aware of the potential for misuse and are responsible for explaining to pupils, the expectation we have of them. Teachers will have access to pupils' emails and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met.
- Pupils will be guided to sites in lessons that have been checked as suitable and processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Pupils will be monitored when using the Internet when they are allowed to freely search, e.g. using search engines. Staff should be vigilant in monitoring the content of the websites the young people visit and they are expected to use age-appropriate search tools.
- The school never allows 'raw' image search with pupils e.g. Google image search.
- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the Click On IT helpdesk via the E-Safety Co-ordinator or network manager.
- The school will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- There will be a 'no blame' environment that encourages pupils to tell a teacher or other responsible adult immediately if they encounter any material that makes them feel uncomfortable.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

  As part of the Computing curriculum, pupils are taught:

- to be critically aware of the materials and content they access on-line and to validate the accuracy of information;
- to know how to narrow down or refine a search;
- to be aware that the author of a website or page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- to understand the issues around aspects of the commercial use of the Internet, as age-appropriate. This may include, risks in pop-ups; buying online; online gaming or gambling;
- what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher.

6. Acceptable Use Policy and G Suite for Education Agreement

These Policies take the form of clear rules to which children, parents and staff indicate their agreement.

The AUP Policy reflects the use and responsibility of each group and their ability to take responsibility for their own use of the technology. There are therefore separate agreements for:

- Children
- Members of staff

Parents and children in are also required to agree to a G Suite for Education Agreement.

(Refer to AUP and G Suite for Education Agreement in E-Safety Handbook)

7. Use of Digital and Video Images

- When using digital images, staff are expected to inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- Members of staff are allowed to take digital or video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. **Such images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.**
- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
- Photographs published on the Website and Twitter, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on the School Website, in association with photographs.
- Permission from parents will be obtained before photographs of pupils are published on the School Website
- A designated member of School staff will maintain the School's Twitter account, as agreed by the Chair of Governors. They will follow the following protocol: tweets will only happen during school hours and the images will be deleted from their device.

As part of the Computing curriculum, pupils are taught:

- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
- to understand why they must not post pictures or videos of others without their permission;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention.

8. Use of Email

- From Key Stage 2 (Year 4) onwards pupils may use LGfL 'Safemail' on the School system.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Access in school to external personal email accounts may be blocked.
- The forwarding of chain letters is not permitted.
- Pupils are introduced to, and use email as part of the Computing scheme of work.

As part of the Computing curriculum, pupils are taught:

- not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent;
- that an email is a form of publishing, where the message should be clear, short and concise;
- that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- that they must not reveal private details of themselves or others in email, such as address, telephone number, etc.;
- to STOP and THINK before they CLICK and not open attachments unless sure the source is safe;

- that they must immediately tell a teacher or other responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening emails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them.

9. Use of Social Networking

The School blocks access to social networking sites and newsgroups unless a specific use is approved.

As part of the Computing curriculum, pupils are taught:

- never to give out personal details of any kind which may identify them or their location;
- not to place personal photos on any social network space;
- to set passwords, deny access to unknown individuals and block unwanted communications;
- to invite known friends only and deny access to others;
- to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.

10. Filtering Policy

The filtering of Internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. No filtering system can guarantee 100% protection against access to unsuitable sites. It is therefore important that the School has a policy regarding filtering to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Belmont is part of the Hounslow LGfL network and, in common with other connected organisations in the Local Authority, automatically receives the benefits of a managed filtering service, with some flexibility for changes at local level.

10.1 Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the E-Safety Co-ordinator who will decide whether to make school level changes. If it is felt that the site should be filtered (or unfiltered) at LGfL level, the Network Manager should click on the Send Comment button on the web page brought up when the site is blocked.

10.2 Monitoring

As the filtering system cannot guarantee 100% protection, the School monitors the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Policy. Monitoring will take place as follows:

10.3 Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the Head Teacher
- E-Safety Governor and/or Community Committee

The Filtering Policy will be reviewed in response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring and/or disciplinary action might be necessary).

11. Password Security

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access;
- no user is able to access another's files, without permission (or as allowed for monitoring purposes within the School's policies);
- access to personal data is securely controlled in line with the School's policy (see section 12 below);
- logs are maintained of access by users and of their actions while users of the system ;

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems, including email.

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access or data loss. This should apply to even the youngest of users, even if class logons are being used.

12. Data Protection/ GDPR

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

Please refer to the Data Protection and GDPR Policy for further detail.

Sensitive data will be transferred using encryption and secure password protected devices only. (The Local Authority has a secure system for transfer of pupil data to and from schools and other services e.g. admissions, Social Care). Any data must be securely deleted from devices and secure sites, in line with school policy once it has been transferred. The School will monitor its use of portable computer systems, USB sticks or any other removable media, to ensure that any sensitive data cannot be linked to an individual unless the data is encrypted and password protected.
(Please refer to the School's Data Protection and GDPR Policy).

13. Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this Policy. However, there may be times when infringements of the Policy could take place, through careless or irresponsible use or, very rarely, through deliberate misuse.
For the handling of e-safety infringements the flow chart should be consulted and actions followed in line with it (refer to Flowchart for Responding to E-Safety Incidents in E-Safety Handbook), the Handbook lists the responses that will be made to any apparent or actual incidents of misuse:

If a pupil infringes the E-Safety Policy the incident will initially be referred their Team Leader. After repeated misuse, access to computers and/or the Internet in school may be removed for a specific time. Refer to Dealing with Pupil Incidents table (E-Safety Handbook) for how different incidents will be handled.

If a staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the Head Teacher. Refer to Dealing with Staff Incidents table (E-Safety Handbook) for how different incidents will be handled.

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The incident must be immediately reported to the Head Teacher, who will seek advice from the Local Authority and report to the police and Social Services as advised. Evidence should be preserved to assist investigation.

14. Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (See Safeguarding and Child Protection Policy)
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

15. Monitoring and Review of the Policy

- This Policy will be reviewed annually as part of the school's E-Safety Audit and referred to the governors' Community Committee should changes be necessary.
- The Head Teacher will report annually on e-safety and the implementation of this Policy to the Governing Body.

PART TWO - HANDBOOK

1. Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of E-Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from LGfL, including the effective management of content filtering.

2. Education and Training

2.1 Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this Policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- The E-Safety Co-ordinator will receive regular updates through attendance at LA training sessions and by reviewing guidance documents released by LA and others.
- This E-Safety Policy and its updates will be presented to and discussed by staff.
- The E-Safety Co-ordinator will provide advice, guidance and/or training as required to individuals as required.

2.2 Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any group involved in ICT, e-safety, health and safety, child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation.
- Participation in school training and/or information sessions for staff or parents

3. Communication

3.1 Good Practice

When using communication technologies the school considers the following as good practice:

- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents (email, chat, video etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

3.2 Communication Grid

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school *currently* considers the benefit of using these technologies for education outweighs their risks or disadvantages. This grid is subject to review each year.

	Staff and other adults				Pupils			
Communication technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with permission	Not allowed
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons		✓						✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones or other personal devices			✓					✓
Use of hand held devices e.g. PDAs, PSPs		✓					✓	
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails		✓	✓			✓		
Use of chat rooms /facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs in school time				✓				✓
G Suite for Education	✓				✓			
Video tutorials/ meetings	✓					✓		

4. Unsuitable/Inappropriate Activities

Some Internet activity e.g. accessing child abuse images or distributing racist material is illegal and all such activity is obviously banned from the School and all other ICT systems. Other activities e.g. cyber-bullying are also banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

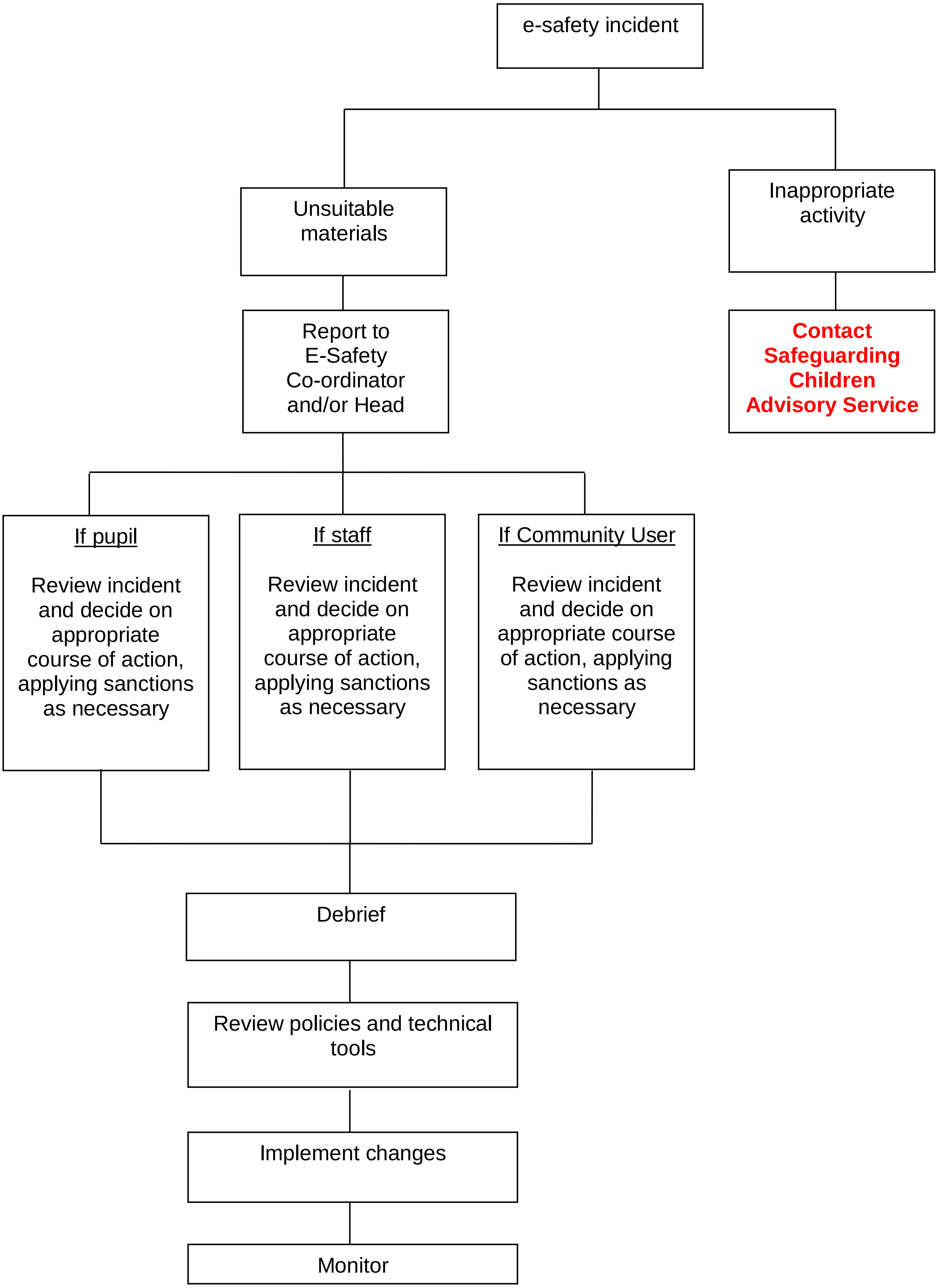
The school believes that the activities referred to in the following section would be inappropriate in a school context and those users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain Internet usage as listed in the following table:

5. Restricted Internet Usage

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images					X
	Promotion or conduct of illegal acts, e.g. those covered by child protection, obscenity, computer misuse and fraud legislation					X
	Adult material that potentially breaches the Obscene Publications Act in the UK					X
	Criminally racist material in UK					X
	Pornography				X	
	Promotion of any type of discrimination				X	
	Promotion of racial or religious hatred				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LGfL, LB Hounslow and/or the School					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions						X
Revealing or publishing confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)						X
Creating or propagating computer viruses or other harmful files					X	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet					X	
Online gaming (educational)			X			
Online gaming (non-educational)					X	
Online gambling					X	
Online shopping/commerce					X	
File sharing					X	
Use of social networking sites					X	
Use of video broadcasting e.g. YouTube			X			

6. Flowchart for Responding to E-Safety Incidents at Belmont School

Adapted from Becta – e-safety 2005


e-safety incident
Unsuitable materials
Inappropriate activity
Report to E-Safety Co-ordinator and/or Head
Contact Safeguarding Children Advisory Service
If pupil
Review incident and decide on appropriate course of action, applying sanctions as necessary
If staff
Review incident and decide on appropriate course of action, applying sanctions as necessary
If Community User
Review incident and decide on appropriate course of action, applying sanctions as necessary
Debrief
Review policies and technical tools
Implement changes
Monitor

7. E-Safety Audit

This quick self-audit will help the senior leadership team (SLT) assess whether the e-safety basics are in place.

Has the school got an E-Safety Policy?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated person for Child Protection is:	
The E-Safety Co-ordinator is:	
Has e-safety training been provided for both pupils and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign an ICT Acceptable Use Policy Agreement?	Y/N
Do parents agree that their child will comply with the School e-safety rules?	Y/N
Have school e-safety rules been set for pupils?	Y/N
Are these rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act/ GDPR?	Y/N

8. Dealing with Pupil Incidents

Pupils	Actions/Sanctions							
Incidents:	Refer to class teacher	Refer to Head Teacher	Refer to Police and/or Social Services	Refer to network manager	Inform parents	Warning	Removal of network/ access/rights to Internet	Further sanction e.g. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in Restricted Internet Usage table)		✓	✓		✓			As advised by LA/police
Unauthorised use of non-educational sites during lessons	✓					✓		
Unauthorised use of mobile phone/digital camera/other hand held device	✓	✓			✓	✓		
Unauthorised use of social networking/instant messaging/personal email	✓	✓			✓	✓		
Unauthorised downloading or uploading of files	✓	✓		✓	✓	✓		
Allowing others to access school network by sharing username and passwords	✓				✓	✓		
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓			✓	✓		
Corrupting or destroying the data of other users	✓	✓			✓	✓		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓			✓	✓	✓	
Continued infringements of the above, following previous warnings or sanctions	✓	✓			✓		✓	✓
Actions which could bring the school into disrepute or breach of integrity of the ethos of the School	✓	✓			✓	✓	✓	✓
Using proxy sites or other means to subvert the School's filtering system	✓	✓		✓	✓	✓	✓	✓
Accidently accessing offensive or pornographic material and failing to report the incident	✓	✓			✓	✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	As advised by LA/police
Receipt or transmission of materials that infringes the copyright of another person or infringes the Data Protection Act	✓	✓			✓	✓		

9. Dealing with Staff Incidents

Staff	Actions/Sanctions							
Incidents:	Refer to line manager	Refer to Head Teacher	Refer to Police	Refer to network manager	Refer to LA	Warning	Disciplinary action	Suspension
Excessive or inappropriate personal use of the Internet/social networking sites/instant messaging/personal email	✓					✓		
Unauthorised downloading or uploading of files		✓		✓		✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓				✓	✓	
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓							
Deliberate actions to breach data protection or network security rules		✓			✓	✓	✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓		✓		✓	✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓			✓		✓	
Using personal email/social networking/instant messaging/text messaging to carry out digital communications with pupils		✓			✓		✓	
Actions which could compromise the staff member's professional standing		✓				✓		
Actions which could bring the school into disrepute or breach of integrity of the ethos of the school		✓				✓	✓	
Using proxy sites or other means to subvert the school's filtering system	✓	✓		✓		✓	✓	
Accidently accessing offensive or pornographic material and failing to report the incident	✓	✓		✓		✓		
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓	✓		✓	✓
Breach copyright or licensing regulations	✓	✓		✓		✓		
Continued infringements of the above, following previous warnings or sanctions		✓	As advised by LA		✓		✓	✓
Deliberately accessing or trying to access other material that could be considered illegal (see list in Restricted Internet Usage table)	✓	✓	As advised by LA	✓	✓	✓	✓	

10. Technical – infrastructure / equipment, filtering and monitoring:

The School will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this Policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually.
- All users will be provided with a username and password by the Network Manager who will have access to an up to date record of users and their usernames.
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head Teacher.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and E-Safety Co-ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.
- An appropriate system is in place for users to report any actual/potential e-safety incident to the Network Manager or E-Safety Co-ordinator. The log is to be found with the E-Safety Co-ordinator
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of ‘guests’ (e.g. supply or trainee teachers or visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files by users
- An agreed policy is in place that forbids staff from installing programmes on school workstations or portable devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations or portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the Internet or taken off the school site unless safely encrypted or otherwise secured.

11. Acceptable Use Policies

See following pages

Note -this form will now be Completed online with Google forms

BELMONT PRIMARY SCHOOL
Inspire ~ Nurture ~ Flourish

Pupil Acceptable Use Policy

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will only look at or delete my own files.
- I understand that I must not bring software or removable storage devices into school without permission, including smart watches that include cameras.
- I will not give my home address or phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not use Internet chat rooms or instant messaging services.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it, but I will show a teacher / responsible adult.
- I am aware that some websites have age restrictions and I should respect this.
- I understand that the school may check my computer files and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

BELMONT
PRIMARY SCHOOL
Inspire ~ Nurture ~ Flourish

Pupil Acceptable Use Policy

Email address

Child’s forename

Child’s surname

Child’s class

Parent/Carer’s Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. I understand that any photographs/ videos that I take at school events should be for my own personal use and will not publish online anything that could identify children other than my own.

□ I agree

Parent/ Carer’s Consent for Web Publication of Work

If selected, my son/daughter’s work may be published on the school website.

□ I agree

□ I disagree

Parent/ Carer’s Consent for Web Publication of Photographs

If selected, photographs that include my son/daughter can be published on the school website, subject to the school policy that names are not published alongside photographs, without further permission being sought.

□ I agree

□ I disagree

Parent/Carer's Consent for use of Photographs within the school community including parent newsletters

□ I agree

□ I disagree

Parent/Carer's consent for the publication of photographs on third party websites

If selected, photographs that include my son/daughter can be published on the website concerned, subject to the school policy that names are not published alongside photographs, without further permission being sought.

□ Yes

□ No

By ticking the box, I agree that this has been read and discussed with my child.

□ I agree

NB: This will be completed online

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the head teacher and governing body.
- I will not reveal my password(s) to anyone.
- I will not allow unauthorised individuals to access email, Internet, intranet, network or other school / LA systems.
- I will ensure all documents, data etc. are saved, accessed and deleted in accordance with the school's policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
  (This is currently: LGfL)
- I will only use the approved school email, School Website or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Computing coordinator or, in her absence, the head or deputy.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network or Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission from the head teacher and will not store images at home without her permission.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any 'significant personal use' as defined by HM Revenue & Customs.

- I will access school resources remotely (such as from home) only through the LGfL / school approved methods and follow e-security protocols to access and interact with those materials.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the head teacher as designated person for child protection or, in her absence, the deputy head.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): Staff agreement form

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the network and Internet; and be able to use the school's ICT resources and systems.

□ I agree

G Suite for Education permission letter

Dear Parents and Carers,

As a school, we introduced Google's 'G Suite for Education' last year as a learning tool and we will continue to use it this year both within school and as an integral part of our remote learning offer for children in all year groups.

In order to keep you informed and also to comply with data protection legislation and Google's Terms of Service, we are required to get parental permission annually for each child to use G Suite. Google's T's and C's can be viewed here: http://goo.gl/D9GNB6

G Suite for Education is an essential part of the curriculum, for all subjects, and **pupils without parental permission will be unable to participate in any lessons across the curriculum using G Suite for Education.** School staff will monitor the use of G Suite for Education when pupils are at school. Parents and carers are responsible for monitoring their child's use of applications when accessing G Suite for Education from home.

Please click the following link to give your permission. The form will only take a couple of minutes to complete.

https://docs.google.com/forms/d/e/1FAIpQLSe3Gqum4WeVWKzWSneo_3n7mgQKviXccai-4JYyZDAeme8HLA/viewform?usp=sf_link

The following form is completed online

Following these simple rules will help school to keep you safe:

- At all times, I will think before I click (especially when deleting or printing).
- When using the internet, I will think about the websites I am accessing.
- If I find a website or image that is inappropriate, I will turn off the monitor and I will tell my teacher straight away.
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site.
- I know that the Internet is provided for pupils to find information, practice skills and communicate with others. It is not for online gaming outside of lessons.
- Internet access is a privilege, not a right and that access requires responsibility. Unauthorised use of the Internet or use of unauthorised websites will not be tolerated. Individual users of the Internet are responsible for their behaviour and communications over the network.
- When communicating online (in blogs, email etc.) I will think about the words that I use and will not use words that may offend other people.
- Pupils should not expect that files stored on school servers or disks will always be private. When communicating online, I will only use my first name and not share personal details such as my email address or phone number.
- The school has its own system for filtering individual websites. Any member of the school community can bring a website which causes them concern to the attention of the Computing Coordinator who can arrange for that site to be blocked in school.
- I understand that people online might not be who they say they are.
- I will not look at other people's files or documents without their permission.
- I will not logon using another person's account (with or without their permission.)
- I will think before deleting files and I will ask a teacher before printing any document.
- I know that the teachers can, and will, check the files and websites I have used and visited. I know that, when using G Suite for Education, teachers can and will check the emails that I send and receive. I will take care when using the computers and other school equipment.

- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers but NOT other pupils.
- I will not install any software or hardware (including memory sticks) without permission from a teacher.

I understand that if I am acting inappropriately or don't follow the rules my access to some or all ICT resources can be suspended. A child who is unable to follow the above rules will be dealt with in accordance with the school's Behaviour Policy. Keep a copy of this at home, perhaps near your home computer.

Email address:
Child's forename:
Child's surname:
Child's class:

ICT Usage Policy and Agreement

Pupil: I agree to the above ICT usage policy and agreement rules and understand the consequences for not following them.

Parent: I give my consent for my child to use G Suite for Education and the internet in school. I fully support the school and will promote good digital citizenship at home. I understand that my child is responsible for their own ICT use in school.

□ I agree □ I disagree

By ticking the box, I agree that this has been read and discussed with my child. □ I agree

Password Protocol

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Network Manager and E-Safety Co-ordinator.

All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames. Users will be required to change their password periodically or immediately if a breach of security is suspected

The following rules apply to the use of passwords:

- Staff user passwords must be changed regularly.
- Pupil user passwords will be kept at class levels until the class teacher is confident the pupils can progress to individual passwords, at which time the staff user rule above will apply.
- The account will be 'locked out' following six successive incorrect logon attempts.
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log on.
- Passwords will not be displayed on screen, and will be securely hashed (use of one-way encryption)
- Passwords can be changed by the individual user by pressing Ctrl + Alt + Delete simultaneously and clicking on the Change Password button.
- The 'master / administrator' password/s for the school ICT system, used by the Network Manager is/are also available to the Head Teacher and kept in the school safe. This/these administrator level passwords must be treated at all times with the utmost confidentiality and NOT passed onto anyone other than the Head Teacher or Network Manager. Any breach must be flagged to Head Teacher and Network Manager immediately for further action to be taken and for those passwords compromised to be changed

The Network Manager and E-Safety Co-ordinator will ensure that full records are kept of:

- User IDs and requests for password changes
- User logons

- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information will be given the highest security classification and stored in a secure manner.

These records will be reviewed by the E-Safety Co-ordinator, E-Safety Governor and Network Manager termly.

This policy will be annually reviewed in response to changes in guidance and evidence gained from the logs.

13. The Benefits of Internet Use

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DFE; access to learning wherever and whenever convenient.

14. Useful links

Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

London Grid for Learning
http://www.lgfl.net/esafety/Pages/safeguarding.aspx

Child Exploitation and Online Protection Centre (CEOP)
http://www.ceop.gov.uk/

ThinkUKnow
http://www.thinkuknow.co.uk/

CHILDNET
http://www.childnet-int.org/

INSAFE
http://www.saferinternet.org/ww/en/pub/insafe/index.htm

Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:
http://www.mmiweb.org.uk/publications/ict/esafetyks1and2.pdf

“Safeguarding Children in a Digital World”
http://webarchive.nationalarchives.gov.uk/20101102103654/publications.becta.org.uk//display.cfm?resID=35446

Kent NGfL
http://www.kented.org.uk/ngfl/ict/safety.htm

National Education network
NEN E-Safety Audit Tool: http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html

Cyber-bullying
DFE - Cyberbullying guidance
http://www.kidscape.org.uk/cyberbullying/

Teachernet “Safe to Learn – embedding anti-bullying work in schools”
http://www.abatoolsforschools.org.uk/pdf/SAFE%20TO%20LEARN.pdf

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

East Sussex Council – Cyberbullying - A Guide for Schools:
https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx

Social Networking
Digizen – “Young People and Social Networking Services”:
http://www.digizen.org/socialnetworking/

Mobile Technologies
Data Protection and Information Handling
Information Commissioners Office - Data Protection:
http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

BECTA - Data Protection:
http://webarchive.nationalarchives.gov.uk/20081105151713/foi.becta.org.uk/display.cfm?cfid=1170520&cftoken=75353a58ed02e72a-6d3b4bbc-0a00-454d-edba9b0745a9b559&page=1759

15. Resources

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the “SWGfL Safe” website:
http://www.swgfl.org.uk/staying-safe

Links to other resource providers:

Kidsmart: http://www.kidsmart.org.uk/default.aspx

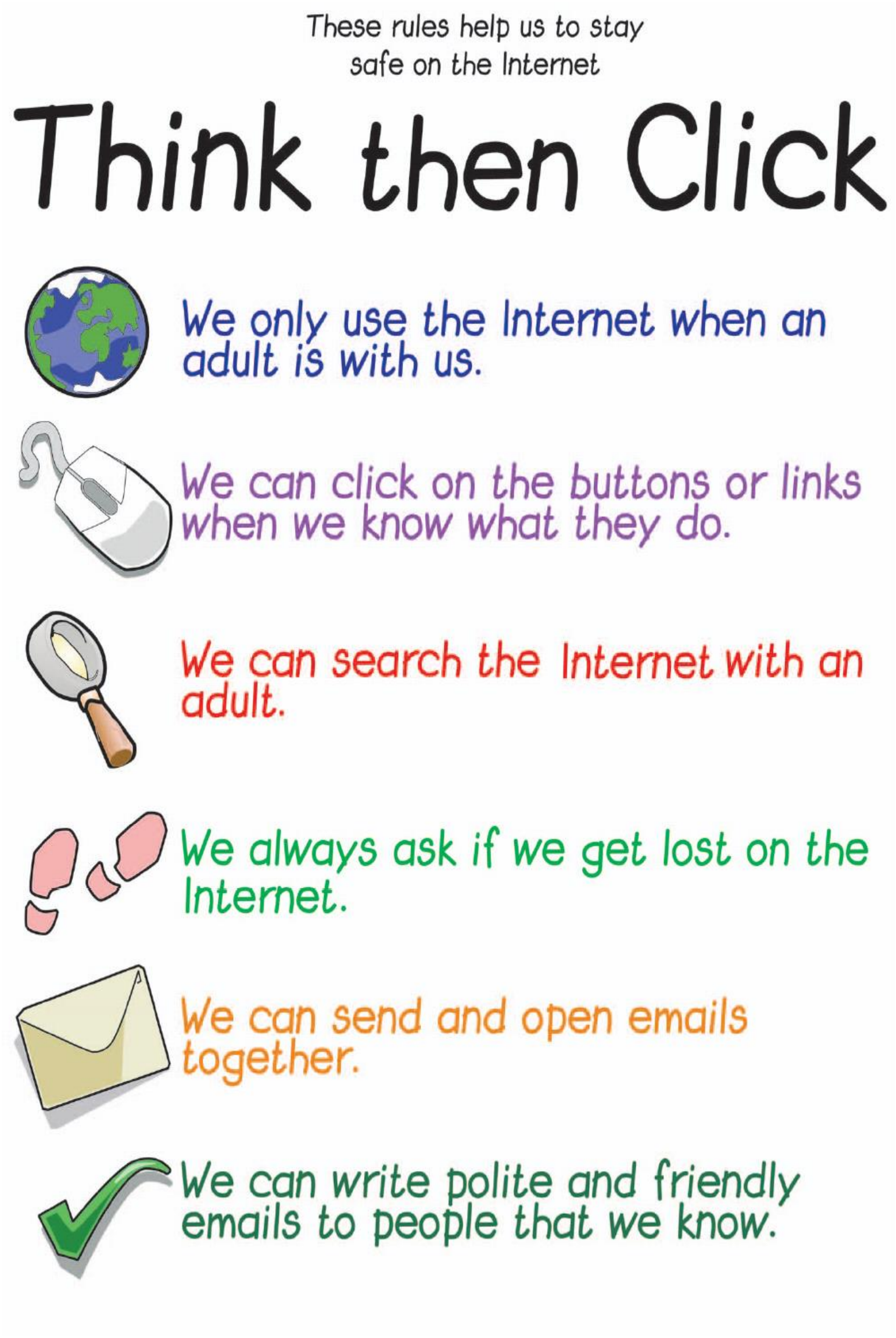
Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

Chatdanger - http://www.chatdanger.com/

Internet Watch Foundation: http://www.iwf.org.uk/

Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx



These rules help us to stay safe on the Internet

Think then Click

We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

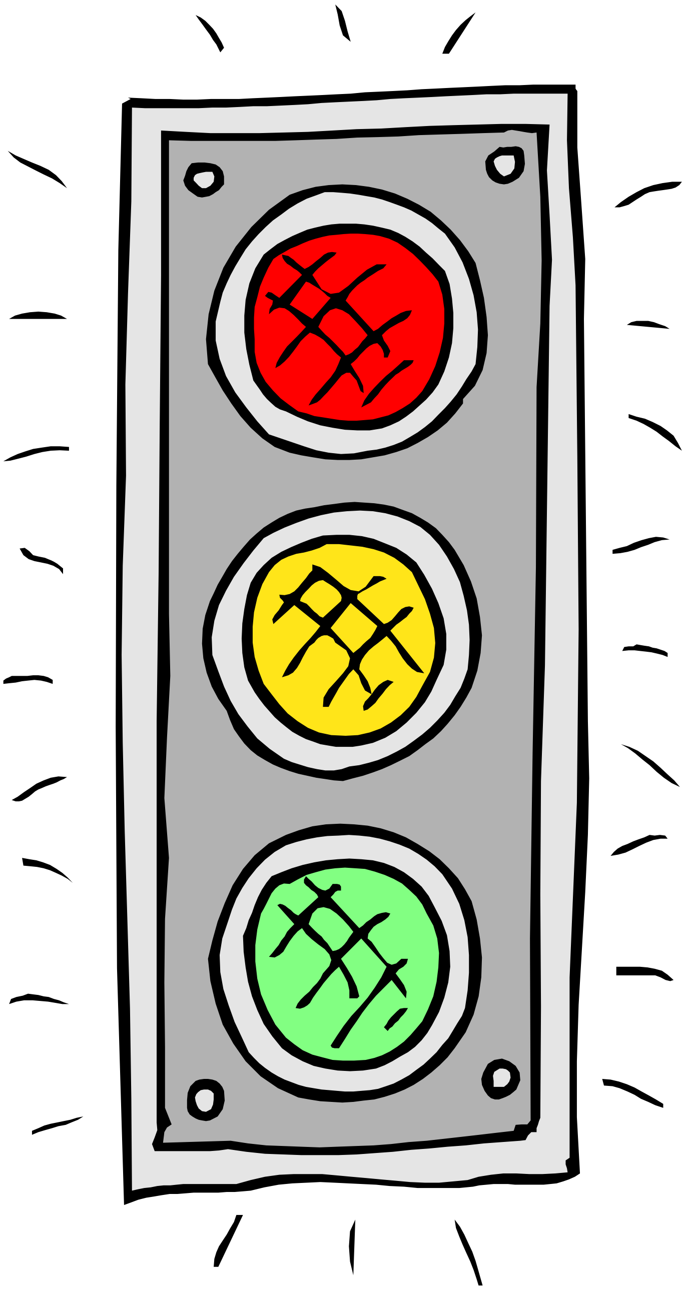
We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Be Internet Safe



Stop

Think

Click

Think then Click